# EXHIBIT E

Excerpts from Declaration of Geoffrey M. Godfrey in Support of Defendant's Joint Reply Motion for Summary Judgment Regarding Invalidity (D.I. 402)

FILED UNDER SEAL

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF DELAWARE

| | |
|---|---|
| SRI INTERNATIONAL, INC., a California Corporation,<br>Plaintiff and Counterclaim-Defendant,<br>v.<br>INTERNET SECURITY SYSTEMS, INC., a Delaware corporation, INTERNET SECURITY SYSTEMS, INC., a Georgia Corporation, and SYMANTEC CORPORATION, a Delaware corporation,<br>Defendants and Counterclaim- Plaintiffs. | Civil Action No. 04-CV-1199 (SLR)<br><br>**FILED UNDER SEAL THIS DOCUMENT CONTAINS MATERIALS WHICH ARE CLAIMED TO BE CONFIDENTIAL OR RESTRICTED CONFIDENTIAL - CONFIDENTIAL SOURCE CODE AND COVERED BY A PROTECTIVE ORDER. THIS DOCUMENT SHALL NOT BE MADE AVAILABLE TO ANY PERSON OTHER THAN THE COURT AND OUTISDE COUNSEL OF RECORD FOR THE PARTIES** |

**DECLARATION OF GEOFFREY M. GODFREY IN SUPPORT OF DEFENDANT'S JOINT REPLY MOTION FOR SUMMARY JUDGMENT REGARDING INVALIDITY**

I, Geoffrey M. Godfrey, declare as follows:

1. I am a member of the law firm of Day Casebeer Madrid & Batchelder LLP, counsel for Defendant Symantec Corporation. I am admitted to practice law before all courts of the State of California.

2. I make this declaration of my own personal knowledge. If called to testify as to the truth of the matters stated herein, I could and would do so competently.

REDACTED

4. Attached hereto as Exhibit RR is a true and correct copy of selected pages of the 03/09/2006 and 03/10/2006 Deposition of Phillip Porras (hereinafter "Porras Tr.") and the 03/30/2006 30(b)(6) Deposition of Phillip Porras (hereinafter "Porras 30(b)(6) Tr.").

5. Attached hereto as Exhibit SS is a true and correct copy of selected pages of the 05/26/2006 and 05/29/2006 Deposition of George Kesidis (hereinafter "Kesidis Tr.").

REDACTED

8. Attached hereto as Exhibit VV is a true and correct copy of selected pages of the 03/31/2006 Deposition of Peter G. Neumann (hereinafter "Neumann Tr.").

9. Attached hereto as Exhibit WW is a true and correct copy of SRI's Supplemental Response to Symantec's Interrogatories Nos. 12 and 15, dated Dec. 15, 2005.

10. Attached hereto as Exhibit XX is a true and correct copy of SRI's Supplemental Response to Symantec's Interrogatories Nos. 1 and 12 (First Set of Interrogatories), 13 and 15 (Second Set of Interrogatories), dated May 05, 2006.

11. Attached hereto as Exhibit YY is a true and correct copy of pages 19-20 of R.

Bace, INTRUSION DETECTION (Macmillan Technical Publishing 2000).

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct to the best of my knowledge.

Dated: July 10, 2006

By: _____
Geoffrey M. Godfrey

# EXHIBIT RR

# EX. RR

# (PORRAS DEPOSITION EXCERPTS)

# ENTIRE EXHIBIT REDACTED

# EXHIBIT SS

# EX. SS

# (KESIDIS DEPOSITION EXCERPTS)

# ENTIRE EXHIBIT REDACTED

# EXHIBIT VV

# EX. VV

# (NEUMANN DEPOSITION EXCERPTS)

# ENTIRE EXHIBIT REDACTED

# EXHIBIT WW

# EX. WW

# ENTIRE EXHIBIT REDACTED

# EXHIBIT XX

# EX. XX

# ENTIRE EXHIBIT REDACTED

# EXHIBIT YY

# INTRUSION DETECTION

Rebecca Gurley Bace

MTP
MACMILLAN TECHNICAL PUBLISHING U.S.A

# *Intrusion Detection*

Rebecca Gurley Bace

Published by:
Macmillan Technical Publishing
201 West 103rd Street
Indianapolis, IN 46290 USA



International Standard Book Number: 1-57870-185-6

Library of Congress Catalog Card Number: 99-63273

03 02 01 00 7 6 5 4 3 2

Interpretation of the printing code: The rightmost double-digit number is the year of the book's printing; the rightmost single-digit number is the number of the book's printing. For example, the printing code 00-1 shows that the first printing of the book occurred in 2000.

*Composed in Galliard and MCPdigital by Macmillan Technical Publishing*

*Printed in the United States of America*

## Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Macmillan Technical Publishing cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

## Warning and Disclaimer

This book is designed to provide information about intrusion detection. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an as-is basis. The authors and Macmillan Technical Publishing shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

## Feedback Information

At Macmillan Technical Publishing, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us at networktech@mcp.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

PUBLISHER
*David Dwyer*

EXECUTIVE EDITOR
*Linda Ratts Engelman*

MANAGING EDITOR
*Gina Brown*

PRODUCT MARKETING MANAGER
*Stephanie Layton*

ACQUISITIONS EDITOR
*Karen Wachs*

DEVELOPMENT EDITOR
*Katherine Pendergast*

PROJECT EDITOR
*Alissa Cayton*

COPY EDITOR
*June Waldman*

INDEXER
*Larry Sweazy*

ACQUISITIONS COORDINATOR
*Jennifer Garrett*

MANUFACTURING COORDINATOR
*Chris Moos*

BOOK DESIGNER
*Louisa Klucznik*

COVER DESIGNER
*Aren Howell*

COMPOSITORS
*Scan Communications Group, Inc.*
*Amy Parker*

# OVERVIEW

runs on a Sybase database management system, using some of Sybase's internal triggers and other features.

NADIR remains one of the most successful and durable intrusion detection systems of the 1980s and has been extended to monitor systems beyond the ICN at Los Alamos. NADIR continues to monitor the ICN at the time of this publication, and the team continues to modify the system to accommodate new threats and target systems. The principal architect for NADIR is Kathleen Jackson.

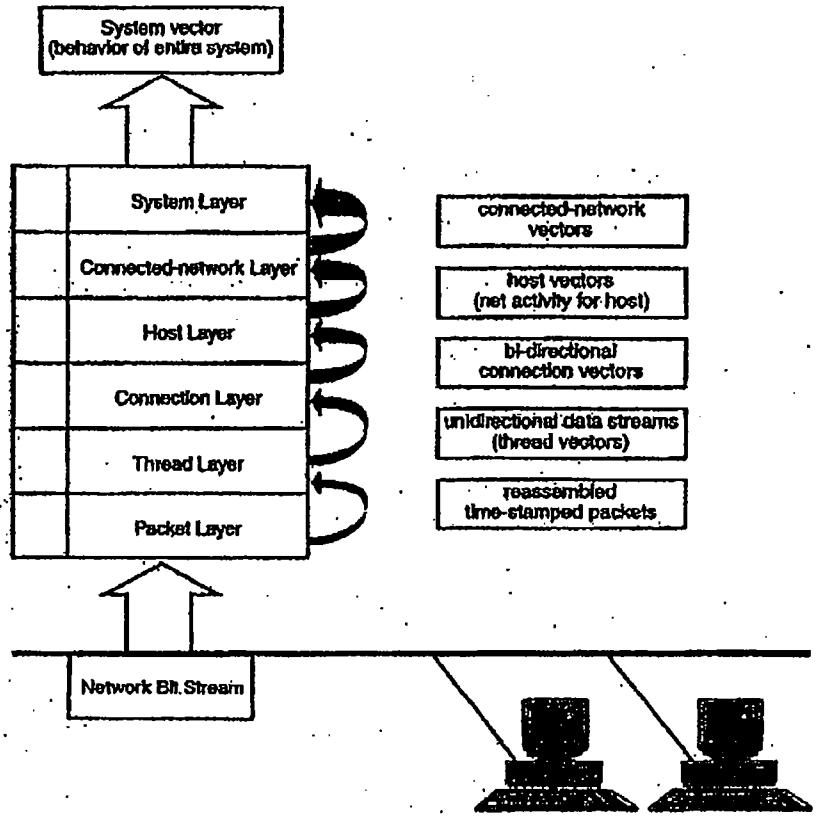
#### *1.2.3.6 NSM*

The Network System Monitor (NSM) was developed at the University of California at Davis to run on a Sun UNIX workstation. It represented the first foray into monitoring network traffic and using that traffic as the primary data source. Before this time, most intrusion detection systems consumed information from operating system audit trails or keystroke monitors. The general architecture of the NSM is still reflected in many commercial intrusion detection products at the time of this publication. The NSM functioned by doing the following:

- Placing the system's Ethernet network interface card into promiscuous mode (in which each network frame generates an interrupt, thereby allowing the monitoring system to listen to all traffic, not just those packets addressed to the system)
- Capturing network packets
- Parsing the protocol to allow extraction of pertinent features as shown in Figure 1.4
- Using a matrix-based approach to archive and analyze the features, both for statistical variances from normal behavior and for violations of pre-established rules

NSM was a significant millestone in intrusion detection research because it was the first attempt to extend intrusion detection to heterogeneous network environments. It was also one of the first intrusion detection systems to run on an operational system (the compiter science department local area network at UC Davis). In a widely cited, two-month test of NSM, it monitored more than 111,000 connections on the network segment, correctly identifying more than 300 of them as intrusions. The system administrators for the network discovered less than one percent of these intrusions. This test emphasized the need for and the effectiveness of intrusion detection systems as part of the protection suite. Principal architects for NSM were Karl Levitt, Todd Heberlein, and Biswanath Mukherjee of the University of California at Davis.[15]

NSM Architecture




### 1.2.3.7 Wisdom and Sense

Wisdom and Sense[16] was an anomaly detection system developed by the Safeguards and Security Group at Los Alamos National Laboratory in partnership with Oak Ridge National Laboratory. Wisdom and Sense was the second pass at an intrusion detection system for mainframes (the initial system, called ALAP, was fielded by the U.S. Department of Energy in several of the department's facilities). Wisdom and Sense operated on a UNIX platform and analyzed audit data from Digital Equipment Corporation VAX/VMS systems. Wisdom and Sense performed statistical, rule-based analyses that were quite different from other systems of the time. The system used *nonparametric techniques* (which are statistical techniques that make no assumptions about the distribution of the data) to derive its own rulebase from archival audit data. Wisdom and Sense then compared subsequent activity to this rulebase, looking for exceptions. The rulebase was structured into